Federal Cloud Security

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

© 2015 The MITRE Corporation.
All rights reserved.

MITRE
December 28, 2015

Katy Warren

NOTICE

This technical data was produced for the U.S. Government under Contract Number HSHQDC-14-D-00006, and is subject to Federal acquisition Regulation Clause 52.227-14, Rights in Data – General, (Deviation 2014).

No other use other than that granted to the U.S. Government, or to those acting on behalf of the US. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.

© 2015 The MITRE Corporation

Approved for Public Release; Distribution Unlimited. Case Number 15-3482

Acknowledgements

Special thanks to Kevin Eiben, CISSP, who provided invaluable technical expertise. This paper would not be possible without his help.

Executive Summary

When Federal government departments and agencies choose to adopt cloud computing, security is a major consideration in the planning, migrating, and operations and maintenance of critical IT systems. Agencies must consider the goals, planned cloud ecosystem, mission and business functions, processes, sensitivity of data, and processing capabilities. Agencies must fully understand the roles and responsibilities of themselves, FedRAMP, and Cloud Service Providers (CSPs). As consumers of cloud services, agencies must also fully understand the impacts of the three Service Models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) with regard to security, as each Service Model brings different security requirements and responsibilities. As agencies transition their applications and data to cloud computing solutions, it is critically important that the level of security provided in the cloud environment be equal to or better than the security provided by its traditional IT environment.

The overall responsibility for securing a system in a cloud computing environment belongs to the agency. However, the day-to-day activities and performance of security controls are distributed between the agency mission owner (who is usually the cloud consumer), users, agency IT security, and CSP. Depending upon the Service Model, the specific division of responsibilities varies. It is necessary to understand roles and responsibilities, and information exchange between the government and CSPs to ensure total system security. CSP responsibilities must be clearly defined in the cloud acquisition and contracts documents.

Most government agencies have a large number of IT systems supporting mission and business functions. Different CSP's will offer different Service Models, and therefore operate under differing security expectations, requirements, processes, and information exchanges. When considering adopting cloud computing, agencies must factor in the simultaneous management of multiple CSP's, and the development of security processes that integrate the management and information flow between multiple CSP's and the government security center. Therefore, understanding the expected cloud ecosystem becomes necessary for the purposes of planning and executing secure cloud computing.

A comprehensive and clear cloud security strategy will provide a needed foundation for securing the agency's cloud adoption. The cloud security strategy should address both technical and non-technical aspects of security, and provide an overall framework for securing the entire cloud ecosystem. It must also ensure security across the responsibility boundaries of the multiple agency organizations, and multiple CSPs. In addition, agencies must evaluate current IT security policies in order to adequately address new cloud technology, and formulate a cloud security strategy that satisfies both the security goals of TIC 2.0 and FedRAMP.

Table of Contents

This page intentionally left blank.

1 Introduction

The goal of this paper is to provide a government cloud consumer with a practical reference regarding current security considerations when adopting cloud computing technologies into the mission, business, and Information Technology (IT) enterprise. This paper provides a list of considerations for decision makers to evaluate security in multiple key areas based on the cloud Service Model and Deployment Model, as defined by the National Institute of Standards and Technology (NIST).

When Federal government departments and agencies (hereafter referred to simply as "agencies") choose to adopt cloud computing, security is, and must be, a major consideration in the planning, migrating, and operations and maintenance of critical IT systems. Agencies must consider the goals, planned cloud ecosystem, mission and business functions, processes, sensitivity of data, and processing capabilities. Agencies must fully understand the roles and responsibilities of themselves, FedRAMP, and Cloud Service Providers (CSPs). Agencies must also fully understand the impacts of the three Service Models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) with regard to security as each Service Model brings different security requirements and responsibilities.

Becoming a consumer of cloud computing includes a transfer of the implementation of many controls to the CSP. While security and privacy concerns when using cloud computing services are similar to those of traditional non-cloud services, concerns are amplified due to external control over organizational assets and the potential for mismanagement of those assets. This potentially includes both information and system components that were previously under the organization's direct control. The transition is usually accompanied by loss of direct control over the management of operations and also a loss of influence over decisions made about the computing environment.

Although direct hands-on security implementation will, to some degree, shift to the CSP, the responsibility for securing systems in the cloud remains with the agency. The loss of direct, day to day, operational implementation and control does not eliminate the agency's security and privacy responsibilities. It just means the agency needs to do things differently. Therefore, the agency must adapt new processes and augment staff skills to perform the necessary CSP oversight to ensure secure operations. The agency consumer must also ensure appropriate integration of the cloud computing services with their own systems for managing security and privacy.

Strong contractual language for cloud services is critical. Although day-to-day operational control of security may, depending on the Service and Deployment Models, be performed by the CSP, the government agency is still responsible for maintaining security and privacy. The shift of direct operational control does not eliminate the agency's responsibilities. The contract between the government agency and the CSP must be clear about the roles of each organization, the duties and responsibilities of each, and how the agency and CSP will manage the relationship and information flow.

Fundamentally, the choice to adopt cloud computing is a business decision. Cloud computing must, first and foremost, be viewed as one of many potential technical solutions to business and mission needs. The *Federal Cloud Computing Strategy*[1] outlines a number of potential cloud advantages. But each government agency must determine their vision and goals, analyze their current and projected IT capabilities and needs, and develop the balance of cloud Service and Deployment Models, and continued traditional IT capabilities that optimize the balance of cost, security, and capability for them. Cloud computing, while potentially powerful, may not be the best solution for every computing need.

1.1 Security-Related Law, Regulation and Policy

Unlike most foreign countries, in the United States, there is no single, centralized, information security or privacy law. A range of Federal laws, regulations, memoranda, guidance and standards impose specific guidance for specific circumstances. Consequently, there are gaps and overlaps in coverage, and they change over time, as new technologies and threats emerge, and counter-measures are developed. The following list demonstrates the variety of IT security provisions (note: this list is not intended to be comprehensive):

- **Federal Trade Commission Act[2]:** Prohibits unfair or deceptive practices -this requirement has been applied to company privacy policies in several prominent cases.
- **Electronic Communications Privacy Act of 1986[3]:** Protects consumers against interception of their electronic communication (with numerous exceptions).
- **Health Insurance Portability and Accountability Act (HIPAA)[4]:** Contains privacy rules applying to certain categories of health and medical research data.
- **Fair Credit Reporting Act[5]:** Includes privacy rules for credit reporting and consumer reports.
- **Gramm-Leach-Bliley Act (GLBA)[6]:** Governs the collection, disclosure, and protection of consumers' nonpublic personal information for financial institutions.
- **Clinger-Cohen Act (CCA)**[7]: Requires every Federal government organization to have a CIO, who is responsible for maintaining information security and privacy.
- **25 Point Implementation Plan to Reform Federal Information Technology Management**: December 2010, U.S. Chief Information Officer (U.S. CIO) Vivek Kundra directed Federal agencies towards a "Cloud First" policy.
- **Federal Cloud Computing Strategy**: February 2011, U.S. Chief Information Officer (U.S. CIO) Vivek Kundra identified benefits of cloud computing, an overall adoption process, and criteria for prioritizing systems migration to cloud.

[1] Vivek Kundra, U.S. Chief Information Officer, *FEDERAL CLOUD COMPUTING STRATEGY*, February 8 , 2011, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

[2] See http://www.law.cornell.edu/uscode/text/15/chapter -2/subchapter- I for details

[3] See http://frwebgate.access.gpo.gov/cgi - bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc18.wais&start=3919965&SIZE=21304&TYPE=TEXT for details.

[4] The final HIPPA regulation and modifications can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

[5] See http://www.ftc.gov/os/statutes/fcradoc.pdf for details.

[6] See http://www.gpo.gov/fdsys/pkg/PLAW -106publ102/content- detail.html for details.

[7] Clinger-Cohen Act, February 10, 1996, including the Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act, 110 STAT. 186 PUBLIC LAW 104–106—FEB. 10, 1996, 104th Congress, Sec. 5131. Responsibilities regarding efficiency, security, and privacy of Federal computer systems.

- **Office of Management and Budget (OMB) Memorandum M-08-05[8] (also known as Trusted Internet Connection (TIC) initiative):** meant to standardize and optimize security of internet connections used by the Federal government. The initiative is intended to improve security posture, monitoring and incident response by reduction and consolidation of external network connections.
  - **TIC Reference Architecture 2.0[9]:** introduces new capabilities and clarifies existing mandatory critical capabilities, including recommended capabilities based on evolving technologies and threats.
- **Federal Information Security Management Act of 2002**[10] (FISMA; 44 U.S.C. §§ 3541-3549), OMB Memos 10-15 and 10-28: requires federal agencies to implement a security program for the agency's information systems. It uses a "risk-based policy," and requires agencies to conduct and report annual information security program review results to OMB.
- **Federal Information Security Modernization Act of 2014**[11]: authorizes DHS to assist the administration of agency security practices, coordinating across the federal government, and providing assistance to agencies. DHS is also tasked with overseeing "binding operational directives," or "compulsory direction" to an agency "for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability or risk."
- **National Institute of Standards and Technology (NIST)**: FISMA required NIST to create the standards (FIPS 199 and FIPS 200) and the guidance (suite of Special Publications (SP), including 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations.").
  - SP 800-53 provides a minimal baseline of security controls by categorization level, a part of the Risk Management Framework (RMF).
  - Risk Management Framework (RMF)[12] is the overall information security framework for the entire federal government. It is designed to improve security, strengthen risk management process, and encourage coordination on federal information security.
- **Best Practices for Acquiring IT as a Service**: February 2012, A joint publication of the CIO Council and Chief Acquisition Officers Council. Provides Federal agencies more specific guidance in effectively implementing the "Cloud First" policy by focusing on ways to more effectively procure cloud services within existing regulations and laws.
- **Federal Risk and Authorization Management Program (FedRAMP)**: A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP's approach includes:
  - *Security Assessment*: in accordance with FISMA, Agencies should use NIST 800-53 controls to grant security authorizations

[8] https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf, Clay Johnson III, November 20, 2007, OMB Memorandum M-08-05, Implementation of Trusted Internet Connections (TIC),

[9] http://www.dhs.gov/trusted-internet-connections

[10] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[11] https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

[12] https://rmf.org/index.php/what-is-rmf.html

- *Leveraging and Authorization*: agencies leverage FedRAMP security authorization packages to grant a security authorization at their agency.
- *Ongoing Assessment & Authorization*: ongoing assessment and authorization activities must be completed to maintain the security authorization.

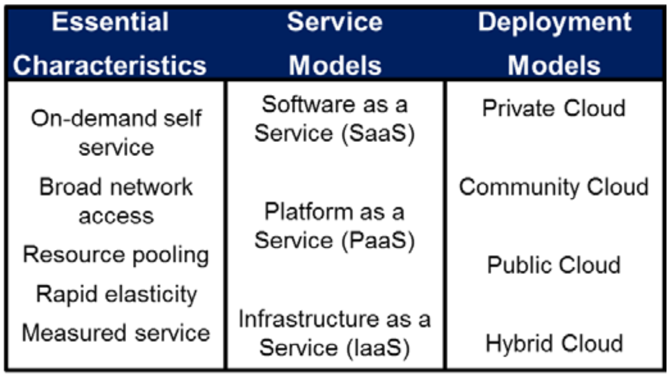
Organizations and programs such as NIST and FedRAMP are working to harmonize and de-conflict standards and guidance with regard to cloud computing in the Federal sector. However, the ultimate responsibility for securing and safeguarding agency information is the agency itself.

2 Cloud Computing

2.1 Definition of Cloud Computing

The NIST SP 800-145 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This cloud model is composed of five Essential Characteristics, three Service Models, and four Deployment Models:

Table 2-1. Definition of Cloud Computing



Essential Characteristics	Service Models	Deployment Models
On-demand self service Broad network access Resource pooling Rapid elasticity Measured service	Software as a Service (SaaS) Platform as a Service (PaaS) Infrastructure as a Service (IaaS)	Private Cloud Community Cloud Public Cloud Hybrid Cloud

Further explanations of the characteristics and models is provided in the following sections.

2.1.1 Essential Characteristics

- **On-demand self-service**. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each service provider.
- **Broad network access**. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- **Resource pooling**. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity**. Capabilities can be quickly provisioned and released on an as needed basis, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, reported, and invoiced, providing transparency for both the provider and consumer of the utilized services.

2.1.2 Service Models

- **Software as a Service (SaaS)**. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform as a Service (PaaS)**. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS)**. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Figure 2-1 illustrates the stack of services, and the responsibilities for providing those services based on the Service Model. In the Government Owned/Government Operated (GO/GO) model, the government provides on-premise or data center infrastructure, operating systems (O/S), data and applications, and security processes for users. For IaaS, a CSP provides essential compute and storage resources, and network access to the consumer. At the PaaS level, runtime, middleware, and virtual operating systems are added to the infrastructure. At the SaaS level, all the necessary software, platform and infrastructure is available to make the system fully functional. Data may be based on usage (e.g. email), or be provided as part of the capability (e.g. roadmaps). In all cases, the appropriate use of the system, security approvals and access rights for users, and oversight of the CSP are the responsibility of the agency consuming the services (indicated by the top-most boxes):

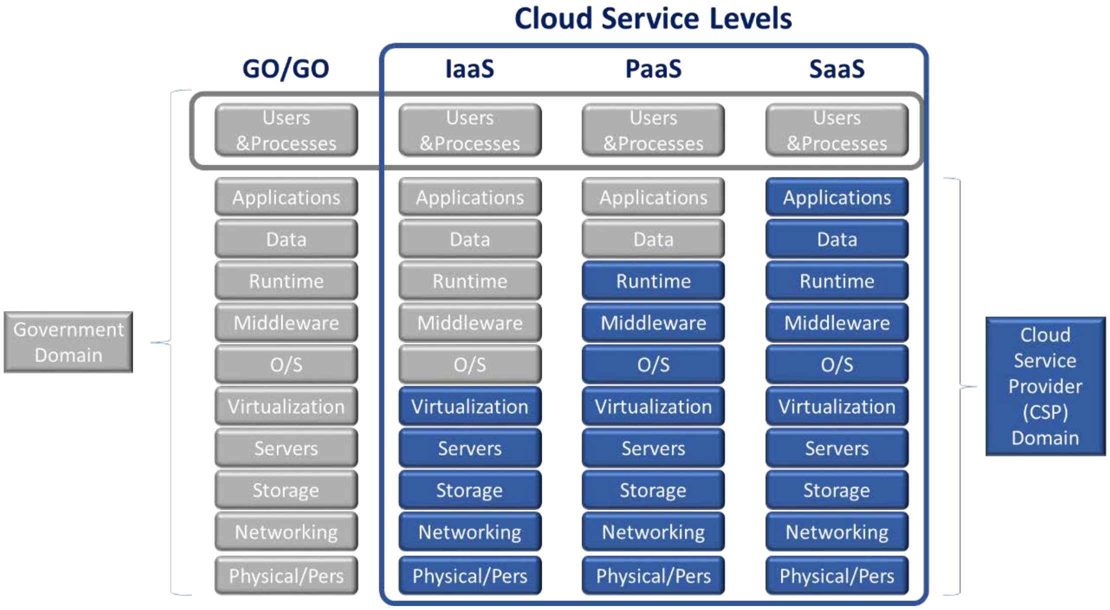


Figure 2-1- Typical Responsibilities Based on Cloud Service Model[13]

2.1.3 Deployment Models

- **Private cloud**. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud**. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

[13] Government owned or government operated (GO/GO) refers to government owned, operated or contracted traditional IT located on-premise, in government owned/operated data centers, or via traditional outsourced IT capabilities

- **Public cloud**. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud**. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."

While several other definitions of cloud types are based on certain characteristics, the general feature of a "hybrid" cloud is its incorporation of a variety of features from the other cloud "types." Generally, agencies operate complex IT environments, and it is likely that a hybrid cloud ecosystem will be required to meet agency needs. This hybrid will potentially exhibit a combination of public, community, and private clouds, which will be further interfaced or integrated with pre-existing on-premise IT.

2.1.4 Cloud Computing Actors

A cloud-computing actor is an entity (e.g., a person or an organization) that plays some role in a process and/or task associated with acquiring, using, developing, managing or operating a cloud-computing instance. As shown and defined in Figure 2-2, below, the NIST cloud conceptual reference model identifies five major actors: Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Carrier, and Cloud Auditor. In addition to these five main cloud-computing actors, the FedRAMP program has identified a sixth actor, known as a Third Party Assessment Organization (3PAO).

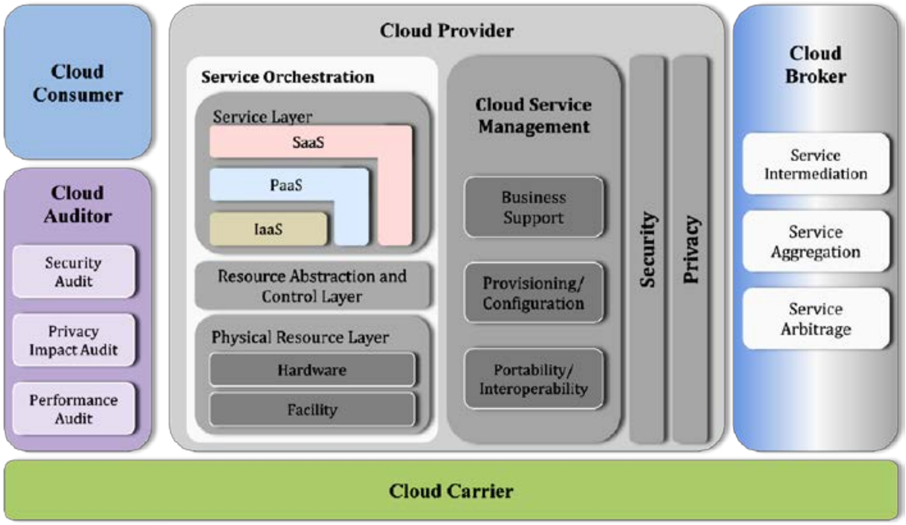


Figure 2-2 NIST Cloud Conceptual Reference Model[14]

[14] NIST SP 500-292, *NIST Cloud Computing Reference Architecture*, September 2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Table 2-2 provides the definitions of each actor and the primary role each plays in cloud computing. These definitions were derived from draft NIST SP 500-299 document on cloud security architecture.[15]

Table 2-2. Cloud Computing Actors

Cloud Actor	Role Description
Cloud Service Consumer (CSC)	A Cloud Service Consumer is the entity that maintains a business relationship with, and uses services from cloud Providers, cloud Brokers, and cloud Carriers.
Provider	A cloud Provider is the entity responsible for making a service available to cloud Consumers (either directly or indirectly via a Broker). A cloud Provider acquires and manages the physical infrastructure that enables cloud services, manages the software that provisions these cloud-computing services, manages operating system and application software (at least for PaaS and SaaS service deployments), and provides cloud Consumers with access to the cloud services by obtaining and managing the appropriate network connections.
Broker	A cloud Broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud Providers and cloud Consumers. Cloud Brokers can provide a method for simplifying the management of multiple cloud services. A cloud Broker may provide one or both of the following services: • Business and relationship support services (business support such as billing and contractual intermediation, arbitrage and aggregation); • Technical support service (service aggregation, arbitrage, and technical intermediation), with a key focus on handling interoperability issues among multiple cloud Providers.
Auditor	A cloud Auditor typically provides an independent assessment of and reports on cloud services. A cloud Auditor evaluates the services of a cloud Provider in terms of security controls, privacy impact, performance, etc. Their reports provide a means to assess a Provider's conformance to standards (e.g., contractual requirements, industry-wide performance measures, and federal guidelines) following a review of objective evidence.
Carrier	A cloud Carrier provides connectivity between cloud Consumers and cloud Providers through network, telecommunications, and other access devices. The security concerns of the Carrier role include consideration of the potential for a breach in confidentiality of data being transmitted to and from a cloud instance.
Third Party Assessment Organizations (3PAO)	A 3PAO independently performs security assessments of the CSP (both the organization and its systems) and creates security assessment package artifacts in accordance with FedRAMP requirements. The 3PAO may also perform continuous monitoring of CSP systems, and hence would then serve in the role of a cloud auditor.

2.2 Virtualization versus Cloud

Confusing IT *out-sourcing*, and *virtualization* with cloud computing is common. Out-sourcing (i.e. contracting for computing capabilities outside the organization), and virtualization (i.e. applying virtual technology such as hyper-visors to infrastructure), are potential elements of cloud computing. Likewise, the Service Model and Deployment Model define *implementations* of cloud computing. However, in order to be a cloud, *all five Essential Characteristics must be in place*. A computing capability may be completely out-sourced to a provider, or completely in-house and "home grown." It may be comprised completely of traditional technology (i.e. no virtualization), or may be fully virtualized (i.e. have virtualized software running on every server). IT services may be provided in a virtual server farm and implement the Service Models (and similar deployment models) using virtual server technology.

[15] NIST SP 500-299 (draft), NIST Cloud Computing Security Reference Architecture, May 2013. http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

In summary, virtualizing a data center is not the same thing as cloud computing. In order to be termed a ***cloud environment***, it must provide the five essential characteristics, as defined by NIST: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

2.3 Assumed Cloud Ecosystem

Most government agencies have a large number of IT systems supporting mission and business functions. Different CSP's will offer different Service or Deployment Models, and therefore operate under differing security expectations, requirements, processes, and information exchanges. When considering adopting cloud computing, agencies must factor in the simultaneous management of multiple CSP's, and the development of security processes that integrate the management and information flow between multiple CSP's and the government security center. Therefore, understanding the expected cloud ecosystem becomes necessary for the purposes of planning and executing secure cloud computing.

For the purposes of this paper, a notional cloud ecosystem has been assumed. As shown in Figure 2-3 the ecosystem includes Office Automation provided as a service (SaaS) by a Cloud Service Provider (CSP). A different CSP provides IaaS and PaaS to the agency for provisioning of multiple mission applications and data necessary to support specific mission processes. These services may be provided by a commercial vendor using a public cloud, or via a community or private cloud. In this scenario the agency is the Cloud Service Consumer.

A shared Identity and Access Management (IAM) capability allows users single sign-on to the entire suite of systems. Business processes determine the use of the systems. Contract, performance, and security oversight of the vendors is provided through central organizations and processes within the agency. A governance program oversees all decisions. The entire ecosystem is compliant with legal regulations and agency policy.

In total, the combined capabilities represent a hybrid cloud, where the agency is consuming services from multiple deployment and Service Models. The agency must also consider the integration of cloud services with on-premise IT systems, and in-house security policy, processes, and controls.

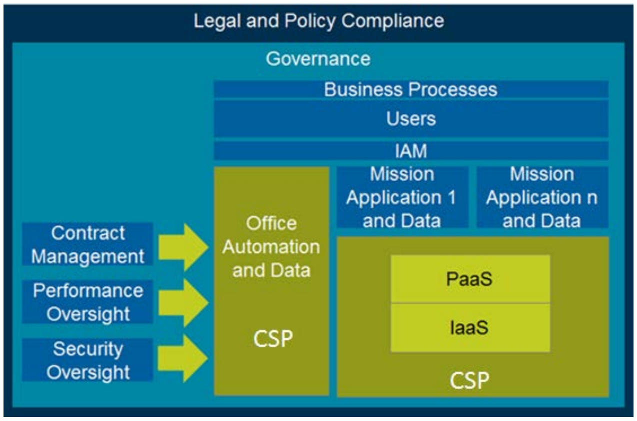

Legal and Policy Compliance
Governance
Business Processes
Users
IAM
Mission Application 1 and Data
Mission Application n and Data
Contract Management
Performance Oversight
Security Oversight
Office Automation and Data
CSP
PaaS
IaaS
CSP

Figure 2-3 Notional Cloud Ecosystem

2.4 Cloud Computing Potential Benefits Summary

There are risks with every type of computing environment, the goal is to manage those risks. While the focus of this paper is on the management of security risks of cloud computing, it is important to note there are numerous potential benefits to adopting cloud computing within an agency. Table 2-3 provides a list of potential benefits that may be realized by an agency, as identified by the Federal Cloud Computing Strategy:

Table 2-3 Cloud Benefits[16]

Cloud Benefits	Current Environment
EFFICIENCY	
Improved asset utilization (server utilization > 60-70%)	Low asset utilization (server utilization < 30% typical)
Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative)	Fragmented demand and duplicative systems
Improved productivity in application development, application management, network, and end-user	Difficult-to-manage systems
AGILITY	
Purchase "as-a-service" from trusted cloud providers	Years required to build data centers for new services
Near-instantaneous increases and reductions in capacity	Months required to increase capacity of existing services
More responsive to urgent agency needs	Lengthy "time-to-market" for new information technology solutions
INNOVATION	
Shift focus from asset ownership to service management	Burdened by asset management
Tap into private sector innovation	De-coupled from private sector innovation engines
Encourages entrepreneurial culture	Risk-adverse culture
Better linked to emerging technologies (e.g., devices)	Slow or lack of adoption for emerging technologies, reducing or eliminating value to agency operations

While security risks need to be identified and managed, use of cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of many organizations. Cloud service providers should be able to offer advanced facilities for supporting security and privacy due to their economies of scale and automation capabilities - potentially a boon to all consumer organizations, especially those who have limited numbers of personnel with advanced security skills.

3 Security Risks

Federal agencies have established security and privacy policies and procedures to protect their sensitive data within the traditional, non-cloud, IT environment. These policies and procedures

[16] Vivek Kundra, U.S. Chief Information Officer, *FEDERAL CLOUD COMPUTING STRATEGY*, February 8 , 2011, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

are developed in accordance with Federal law and policy set forth by OMB, FISMA, and now, FedRAMP.

Cloud security includes an implied organizational division of responsibilities and technologies to enable cloud services. Therefore, cloud computing may present different risks than traditional IT. As part of the transition to cloud computing, it is critical that agencies understand their level of risk tolerance and focus on mitigating the risks based on the sensitivity of information and the risk tolerance level. FedRAMP promotes a risk-based security program based on the evaluation of information sensitivity, and therefore, the necessary and appropriate security and privacy controls to protect said information.

3.1 Security Responsibilities and Cloud

As an agency adopts cloud computing, the vulnerability and sensitivity of business or mission sensitive data, known as Critical Protected Information (CPI), is a critical consideration. Properly addressing the sensitivity and protection of data in the cloud is fundamental to agency data system management. The overall responsibility for securing systems and data in a cloud computing environment belongs to the agency. However, the day-to-day implementation and performance of security controls are distributed between the agency (who is usually the cloud consumer), users, agency IT security, and the CSPs. As necessary, specific security and contract language should be included to clarify the agency's requirements for additional security compliance and the CSP's security operating obligations for data, especially CPI.

Depending upon the agreed to Service Model and Deployment Model, the specific division of responsibilities varies. It is necessary to understand who has responsibility for what, and how information and interaction between the various parties works to ensure total system security. The boundaries between parties must be well understood and managed. CSP responsibilities must be clearly defined in the cloud acquisition documents, contracts, and Service Level Agreements with the CSPs. Consequences for failure to maintain the agreed-upon security levels must also be defined.

In terms of the Service Model, provisioning responsibilities typically reside as indicated in Figure 2-1. Security responsibilities are similarly divided. In a GO/GO environment, such as government data centers or on-premise environments, the agency is responsible for all IT security, and has direct control over all levels of the IT stack, from applications to physical facilities. When cloud is introduced, direct operational agency security control decreases in a step-wise fashion from IaaS (where the CSP provides only infrastructure security), through PaaS, and to SaaS (where the CSP provides total security of application, platform and infrastructure). Above the IT stack, the agency always has security control responsibilities for business processes, users, and security oversight. Note that the agency always has ultimate responsibility for security of information and systems.

Using Figure 2-1 as a basis, the implementation of security controls can be aligned to the stack as shown in Figure 3-1, below. (Note: The list of security responsibilities alignment is not all-inclusive; it is representative of some responsibilities at each level in the stack.) Security responsibility ***always*** rests with the agency, who must ensure that the CSP implements the controls properly.

Further information is included in the following sections.

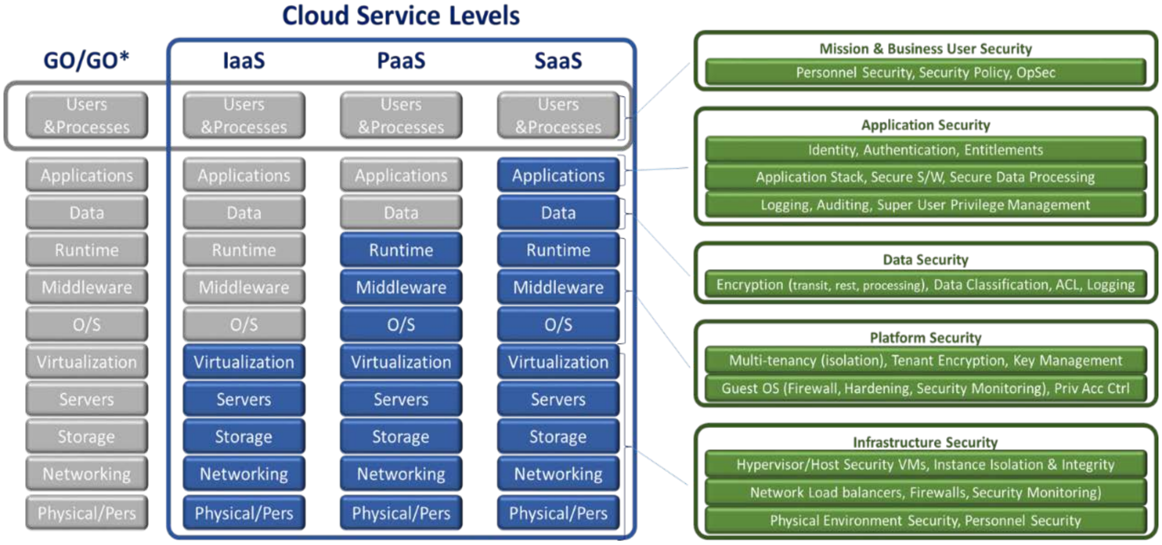

Cloud Service Levels
GO/GO*
IaaS
PaaS
SaaS
Users &Processes
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Physical/Pers
Mission & Business User Security
Personnel Security, Security Policy, OpSec
Application Security
Identity, Authentication, Entitlements
Application Stack, Secure S/W, Secure Data Processing
Logging, Auditing, Super User Privilege Management
Data Security
Encryption (transit, rest, processing), Data Classification, ACL, Logging
Platform Security
Multi-tenancy (isolation), Tenant Encryption, Key Management
Guest OS (Firewall, Hardening, Security Monitoring), Priv Acc Ctrl
Infrastructure Security
Hypervisor/Host Security VMs, Instance Isolation & Integrity
Network Load balancers, Firewalls, Security Monitoring)
Physical Environment Security, Personnel Security

Figure 3-1 Security Consideration Aligned to Cloud Stack

The following diagram summarizes the responsibilities of CSPs and agencies in the IaaS, PaaS and SaaS Service Models. The security boundaries must be well managed for all Service Models.

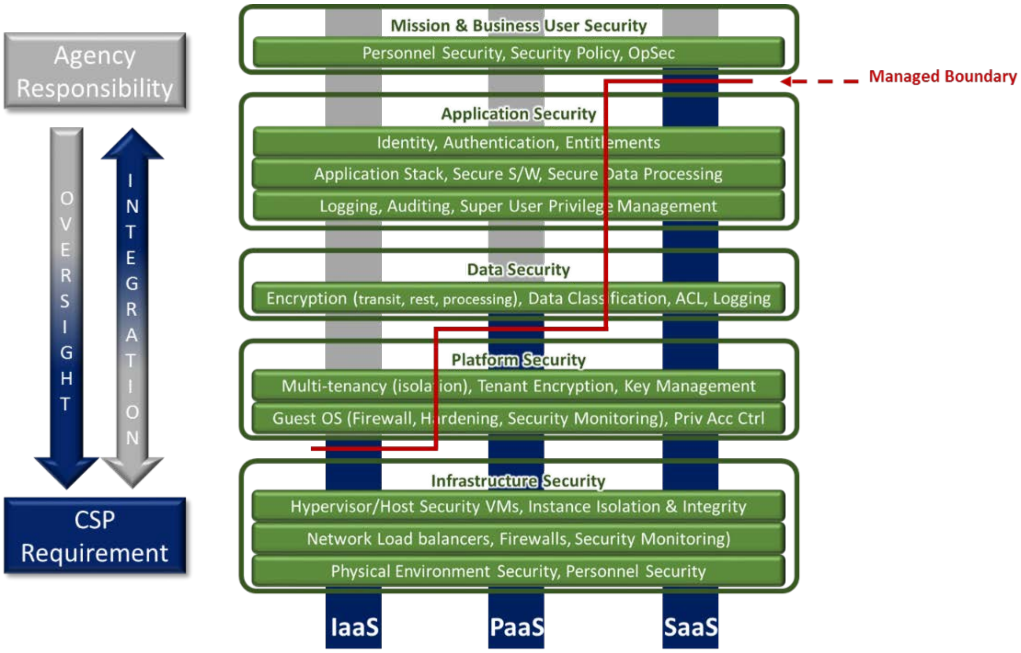

Agency Responsibility
OVERSIGHT
INTEGRATION
CSP Requirement
Mission & Business User Security
Personnel Security, Security Policy, OpSec
Managed Boundary
Application Security
Identity, Authentication, Entitlements
Application Stack, Secure S/W, Secure Data Processing
Logging, Auditing, Super User Privilege Management
Data Security
Encryption (transit, rest, processing), Data Classification, ACL, Logging
Platform Security
Multi-tenancy (isolation), Tenant Encryption, Key Management
Guest OS (Firewall, Hardening, Security Monitoring), Priv Acc Ctrl
Infrastructure Security
Hypervisor/Host Security VMs, Instance Isolation & Integrity
Network Load balancers, Firewalls, Security Monitoring)
Physical Environment Security, Personnel Security
IaaS
PaaS
SaaS

Figure 3-2 – Security Responsibility by Service Model

In order to oversee the security operations of multiple CSPs, it is important for agencies to understand their expected cloud ecosystem, and plan for it. For the sample ecosystem identified in Figure 3-1, the agency must integrate security policy, processes, and procedures with multiple CSPs at multiple Service Models. This will impact the day-to-day relationship, information exchange, reporting, and oversight of the CSPs. The agency's security policies, staff, and processes must be capable of overseeing and integrating the security of all.

The following sections discuss the agency's specific security activities when adopting cloud. As the type of service acquired from the CSP moves down the stack, additional security responsibilities are assumed by the agency consumer. For example, if the agency acquires a SaaS solution, they are (in general) responsible for all mission and SaaS activities. If the agency acquires a PaaS solution, they are still responsible for mission and SaaS, and also responsible for PaaS activities. Table 3-1 summarizes these responsibilities. It is important to note that the following discussion of specific activities is not specific to any CSP. Each CSP may provide security processes or features that extend into other areas of the cloud stack. Each acquisition and contract with a CSP must be addressed individually. ***Security of IT systems and data is always the responsibility of the agency.***

Table 3-1 Agency Security Roles and Responsbilities by Cloud Stack

	If the Government Agency Acquires:		
Specific Security Activities Include:	**IaaS**	**PaaS**	**SaaS**
3.1.1 Mission	Agency	Agency	Agency
3.1.2 SaaS	Agency	Agency	Agency
3.1.3 PaaS	Agency	Agency	
3.1.4 IaaS	Agency		

3.1.1 Mission, Business, Governance & Oversight

Overall security responsibilities reside with the agency cloud consumer regardless of the Service or Deployment Model. These specific activities are the responsibility of the agency at all levels of the cloud stack, regardless of the Service Model (SaaS, PaaS, or IaaS) acquired.[17]

3.1.1.1 Compliance and Legal Risks

Even after a legacy system has received an Authority to Operate (ATO), its risk posture may change by migration to cloud. The risks to the system must be reassessed and mitigation steps implemented, some of which can be covered by using a FedRAMP certified CSP. Agencies can

[17] Note that these are "typical" responsibilities described for informational purposes. Individual CSPs may offer specific security controls at different levels, or may offer options or product packages unique to their offerings.

validate that CSPs have FedRAMP Provisional Authority to Operate (PATO)[18], or establish an agency FedRAMP PATO.

A FedRAMP PATO ensures that a specific CSP offering meets a baseline standard of security for a specified level of sensitivity. For many agencies, this certification may be adequate for most applications. Some agencies (e.g., DoD's FedRAMP+), have established additional security requirements that must also be met by CSPs. In all cases, auditing the CSP will help ensure that processes and security controls are performed and implemented appropriately. The agency has responsibility to verify that the cloud provider has appropriate FedRAMP or agency certifications, and that the security controls implemented by the CSP meet agency requirements. In some cases, as noted above, agencies may require CSPs to implement security controls in addition to those included in the FedRAMP security controls baseline.

3.1.1.2 Loss of Direct Security Control

In adopting cloud, an agency must necessarily cede control to the cloud provider over a number of issues that may affect security. Contracts and Service Level Agreements (SLAs) must establish clear responsibilities and consequences for non-compliance. The terms set forth in the SLA must be designed to support mission objectives, provide clear success measures, including data collection and calculation that measures performance, and consequences. In addition, SLAs provide the opportunity to incentivize CSPs by providing a reward mechanism for outstanding performance, or to encourage innovations and improvements.

3.1.1.3 Responsibility Ambiguity

Given that use of cloud computing services spans across the agency and the CSP organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly. It is also necessary for the agency to be clear about the division of security responsibilities between itself and the CSP and to ensure that the agency's security responsibilities are handled appropriately when adopting cloud. Roles and responsibilities for cloud consumers and providers change in accordance with the type of Service Model (e.g., IaaS versus SaaS). While the agency is responsible for oversight of the CSP, integration of security processes, information, and performance is a mutual ongoing process.

3.1.1.4 Management Interface Vulnerability

CSPs often provide a Web interface for customers to access cloud management and monitoring information, including security data. The CSP may provide access to a large set of information not typically available in a more traditional environment. When combined with global remote access and browser vulnerabilities, this interface becomes a point of security concern. Agencies should manage and monitor this information source, including control of user access privileges, and usage of security information.

[18] All FedRAMP PATO's are considered provisional, as they must be re-issued periodically.

3.1.1.5 Handling of Security Incidents

The detection, reporting and resolution of most security breaches will be performed by the CSP, with oversight from the agency consumer. CSPs must report breaches to the agency; the agency then reports them to the United States Computer Emergency Readiness Team (US-CERT), Congress, and other oversight bodies as required.

Policy, SLAs, and contract terms will provide the basis for security processes and information exchange between the CSP and the agency. However, building a relationship between the agency and CSP will enhance the mutual cooperation and trust, and therefore the handling of security incidents.

3.1.1.6 Security Integration

Most IT systems do not "stand alone." Information and processing capabilities are shared between systems within an agency, between agencies, and with outside parties such as the American people, industry, academia, and even foreign nations. As an agency adopts cloud computing into its IT capabilities, security of the systems and data must be maintained, and improved. When agencies migrate to multiple services from multiple CSP's, security processes within the agency must be adapted to integrate security processes and information exchange to remain effective and efficient. Agency security policy, plans, operations and personnel skills must be reviewed and updated to maximize benefit while simultaneously remaining within risk tolerances. The overall security posture, as implemented by security controls, must be examined to ensure that an integrated security solution is achieved and that controls across multiple Service Models, Deployment Models and CSPs do not introduce vulnerabilities or create performance bottlenecks.

3.1.1.7 Behavior of Insiders

Potential damage by an insider can be substantial. Whether accidentally or maliciously, the damage an insider can cause escalates with the increase in access rights and expertise of the staff. Within a cloud computing environment, such activity might occur from within the agency, the CSP, or both. Contractual requirements to monitor for malicious behavior can help identify it, and SLAs can establish consequences for such insider attacks. However, the CSP's contractual consequences of insider attack, including monetary recompense, may not even begin to repay the mission or agency consequences of the loss of sensitive government data. This added risk must be included in the agency's risk assessment of cloud solutions.

3.1.1.8 Vendor Lock-In

Dependency on a particular CSP could lead to the agency being tied to that particular provider. Despite some claims by CSPs, portability between CSPs is not trivial, automatic, or free. Agencies wishing to migrate from one CSP to another will likely have to fund a project that implements the migration, which will also take time and funding. During this process, agencies face an increased risk of data and service unavailability. The agency should prepare an exit strategy as part of contracting with the CSP. This will enable the agency to plan ahead for continuity of operations in the event of a worst-case scenario.

3.1.1.9 CSP Business Changes

Should a CSP suffer a business failure, it could result in data and applications essential to the cloud consumer's business being unavailable. It could also leave data and applications unprotected by the now-defunct CSP. Similarly, a merger or acquisition of the CSP by another corporation could result in significantly altered security processes that may create new risks or vulnerabilities due to changes in security processes and staffing, changes in the relationship between the agency and CSP, or other unpredictable factors. Well documented security requirements and SLAs in CSP contracts, and open communication with the new CSP, will help to mitigate these issues. While the agency may not exit from the new CSP, the exit strategy may help to guide the change of from the old to the new CSP.

3.1.1.10 Termination of Cloud Services

Should cloud services terminate, regardless of reason, the question of proper data handling arises. CSPs may be legally obligated to retain data and application information for a specified time period. Requests to delete cloud resources may not result in true wiping of the data. If a storage device contains data from multiple cloud consumers, (public or private sector) this is a case of multi-tenancy and hardware reuse, and potentially represents a security risk to the agency.

3.1.2 SaaS (including Data)[19]

This section discusses security concerns for Software as a Service, and assumes the following:

- The agency is the consumer of a SaaS solution whereby the CSP provides the application, data, platform and infrastructure,
- The Deployment Model may be Public, Community or Hybrid, and the agency is not providing the security of the application, platform or infrastructure. (If a Private Deployment Model is used, the agency is responsible for all security at all levels of the cloud stack.)
- Mission and governance security is applied.

If an agency acquires a SaaS solution, implementation of security at the IaaS and PaaS Service Levels will be performed by the CSP. Implementation of the SaaS items outlined in sections 3.1.2.1 – 3.1.2.8 are the generally the responsibility of the agency, or may be shared between the agency and the CSP. The agency performs security oversight, and is still responsible for overall security.

3.1.2.1 User-related Security

Users create security concerns in a SaaS environment, either unintentionally or maliciously. Traditional concerns, such as phishing attacks, continue in SaaS, but cloud also introduces new attack vectors. Identifying normal application usage patterns, or validating that an abnormal usage is not malicious, and is not data exfiltration, will be required. The agency is responsible

[19] Note this is a general discussion for information purposes. Specific cloud service providers may include capabilities, options or product packages that cross the defined boundaries of IaaS, PaaS or SaaS as used in this document.

for setting the policy for user access to the SaaS application. These policies must be clearly communicated to the CSP so that only authorized personnel are granted application access. The procedures for vetting personnel prior to new account creation should be agreed-to by both the CSP and Agency.

3.1.2.2 Identity Services

In order for agency personnel to perform their daily functions, they must be able to access multiple systems in an efficient and timely manner. Some of those systems will be on-premise, and some will be in the form of (possibly multiple) cloud services. A good identity and access management strategy is essential in order to ensure staff are not required to separately log in to every application they use. Therefore, extending identity services into the cloud is necessary for on-demand use of cloud computing services.

3.1.2.3 Authentication

Authentication attacks can be considered a security weak point in virtual services, in part because standards for identity validation and access management are not fully mature. Cloud consumers may not have strong policies for managing and communicating access lists, or may not follow the prescribed procedures. Therefore, authentications attacks tend to be frequently targeted. Phishing attacks are a ripe vector for exploit here. That is, an attacker obtains access to legitimate credentials that are used to access another consumer's environment.

3.1.2.4 Access Control List

Access control regulates who can access what functions and data in an IT enterprise. Validated users are considered to be "authorized." To maintain good security, the agency must provide an Access Control List (ACL) to the CSP outlining the valid users and levels of permission, and maintain that list appropriately. The agency must be diligent about providing and updating the list of valid user credentials to the CSP. ACLs should be reviewed and updated periodically. In addition, certain events should trigger the update of the ACL, such as a new person joining an organization, or a person leaving.

3.1.2.5 Application Stack

The CSP is responsible for providing security of the application stack[20]. The agency must have transparency into the security methods used by the CSP, and the ability to audit the CSP periodically. SLAs must address the security measures and consequences. CSP security reporting and agency oversight of security are critical contracting concerns.

3.1.2.6 Auditing

The agency is responsible for security and privacy policy for application and data protection. Although FedRAMP certification provides a baseline for CSPs regarding securing SaaS capabilities, the agency will be accountable for any additional security requirements. They are

[20] The "application stack" is a set of programs (or "applications") that automate or aid users in an activity. Usually, these programs are components of a business process, or can be closely linked, and may share or exchange data with a minimum of user steps. For example, office applications such as word processing, spreadsheets, and email can be considered an application stack.

also responsible for ensuring that their cloud providers adhere to the policies. Agencies must monitor CSPs routinely, including implementing an audit program that validates the CSPs security program and results.

3.1.2.7 Cloud Systems Inventory

In order to adequately secure systems, the systems first need to be identified and categorized. Recent studies conducted by multiple agency Offices of Inspector General (OIGs) for the Council of the Inspectors General on Integrity and Efficiency (CIGIE)[21] determined that 9 of 19 agencies in the study did not have an accurate and complete inventory of their cloud systems. Without the inventory, the agencies cannot know which data resides outside agency IT boundaries and are subject to the risks associated with cloud. In order to fully and appropriately protect all agency systems, a complete inventory is essential.

3.1.2.8 Data Location and Legal Jurisdiction

A fundamental capability of cloud computing is the ability to utilize available compute and storage devices regardless of physical location. This provides benefits in increase availability and performance, but also raises certain security and legal concerns. It may be difficult at a specific point in time to know where specific data is being processed or is stored. Most Federal agencies contractually restrict data storage and processing to the Continental United States (U.S.).

Before migrating services to a cloud computing environment, it is important to understand the locations provided by CSPs, and the legal consequences. U.S. Federal law imposes select obligations (e.g. data retention, data protection, interoperability, medical file management, disclosure to authorities) that must be met. Ensure the CSP is capable of meeting Federal laws.

3.1.3 PaaS[22]

The subsequent discussion regarding security concerns for Platform as a Service assumes the following:

- The agency is the consumer of a PaaS solution
- The agency is providing software applications and data; including operating, configuring, maintaining and patching
- CSP is responsible for securing the infrastructure and PaaS services
- The Deployment Model can be Public, Community or Hybrid, and the agency is not providing the security of the platform or infrastructure. (If a Private Deployment Model is used, the agency is responsible for all security at all levels of the cloud stack.)
- All security for the SaaS level is applied.

[21] The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the Inspector General Reform Act of 2008, Public Law 110-409. The mission of CIGIE is to:

- Address integrity, economy, and effectiveness issues that transcend individual government agencies; and
- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Federal Inspector General (IG) community.

[22] Note this is a general discussion for information purposes. Specific cloud service providers may include capabilities, options or product packages that cross the defined boundaries of IaaS, PaaS or SaaS as used in this document.

If an agency acquires a PaaS solution, implementation of security at the IaaS Service Level will be performed by the CSP. Implementation of SaaS-level security must be performed by the agency. Implementation of the PaaS items outlined in sections 3.1.3.1 – 3.1.3.6 are generally the responsibility of the agency, or may be shared between the agency and the CSP. The agency performs security oversight, and is still responsible for overall security.

3.1.3.1 Side Channel

A malicious virtual machine placed in close "proximity" to another virtual machine (i.e. the target) could be designed to gain information or side-step isolation mechanisms to infiltrate the target virtual machine. For example, one attack vector is for a malicious cloud consumer to access another consumer's VM or storage through the CSP's hypervisor or other management software.

3.1.3.2 Man-in-the-Middle (Cryptographic Attacks)

If an attacker can interrupt communication between two users, or a user and an application, on a network, it is possible to intercept the data flowing between them. The attacker could siphon information, modify the transmissions, or send false responses to the users or even the application. Encryption while "in transit" makes it harder, although not impossible to perform this type of attack. Periodically changing encryption keys also aids in protecting data in transit.

3.1.3.3 Encryption at Rest

While being stored, data is vulnerable to unauthorized access and exfiltration by "bad actors," external or internal. Further, there are multiple opportunities to access copies of data via databases, redundant Disaster Recovery/Continuity of Operations (DR/COOP) sites, and backups. For data at rest, encryption is often considered as a solution. However, historically, it has been difficult to implement due to management and performance concerns. There are several encryption options, each with different benefits and risks:

- **Application encryption –** The application performs its own encryption and decryption. The database receives and stores pre-encrypted data, and the application decrypts the data for the user. If a communications channel exists between the application and user, then separate encryption of that channel is required.
- **File encryption –** There is a mechanism, possibly through the operating system or a separate security tool, to encrypt files on the storage media. This form of encryption protects only specified files, and does not protect all data on the physical medium. The communications channel from the operating system, through the application, to the user will potentially require separate encryption.
- **Physical Media/Disk encryption –** The operating system supports a mechanism to encrypt database tables or files on the storage media. This option protects the entire physical medium, but may involve performance overhead or configuration complexities.
- **Database encryption –** Some database systems provide the capability for the database to perform encryption and decryption. Selected data or data sets (e.g. data columns) stored in the database and on physical media are encrypted, but decrypted for the application to process. In this option, data exchanges between the database and the

application must be encrypted, decrypted, or both, which adds performance and management overhead.

3.1.3.4 Encryption of Data in Transit

Data in Transit is data that is flowing over a network. The network could be a public (i.e., untrusted) network such as the internet, or a private one such as a Local Area Network (LAN). When accessing a CSP, agencies should assume that data is flowing over an untrusted network.

Data travelling over any network is at risk of being captured and accessed by someone else on the network. For wireless networks, all they need is to be within range. Data in transit can be protected from unauthorized access by encryption. PKI is a common form of encryption for data in transit. However, care must be taken to manage encryption keys effectively.

3.1.3.5 Key Management

The effectiveness of data encryption lies in the security of the encryption keys. The keys must be securely stored and changed routinely. In addition, certain specific events, such as the departure of a system administrator or other key personnel, should also trigger a change in the encryption keys. The procedure for key recovery for individual nodes should be planned and tested so that one node can be placed back on line after an unexpected service outage. In addition, the procedure for an emergency re-key of all nodes should also be determined and practiced.

3.1.3.6 Logs

Logging of processing information and user/support personnel actions is considered standard practice for the majority of IT systems. Cloud is no different. Log files should be considered valuable and sensitive data, and should be subject to the same protections as other sensitive data. Any agency operating in the cloud should ensure they are able to get copies of log files for security operations and other purposes. That will have to be specified in the contract.

3.1.4 IaaS[23]

It is important to note here that because this is the foundation layer of the cloud stack, attack vectors and security concerns related to Infrastructure as a Service apply to all Service Models. The subsequent sections regarding security concerns assume the following:

- The agency is the consumer of an IaaS solution
- The agency is providing all platform capabilities, including provisioning the guest operating system, storage and deployed applications (whether custom developed or software products), including data. The agency performs configuring, maintaining and patching at the platform level in addition to deployed software and data.
- The CSP manages (or controls) the underlying cloud infrastructure, including security for facilities, physical hardware, network infrastructure, and virtualization infrastructure.

[23] Note this is a general discussion for information purposes. Specific cloud service providers may include capabilities, options or product packages that cross the defined boundaries of IaaS, PaaS or SaaS as used in this document.

- The Deployment Model can be Public, Community or Hybrid. (If a Private Deployment Model is used, the agency is responsible for all security at all levels of the cloud stack, including those provided by the CSP for IaaS.)
- All security for the SaaS and PaaS levels are applied.

If an agency acquires an IaaS solution, the CSP will generally perform only infrastructure and networking security up to the hypervisor level. Implementation of the IaaS items outlined in sections 3.1.4.1 – 3.1.2.8 are the generally the responsibility of the agency, or may be shared between the agency and the CSP. Implementation of security at the SaaS and PaaS Service Levels, and overall security, are the responsibility of the agency.

3.1.4.1 Virtualized and Multi-tenant Environments

Multi-tenancy and shared resources are defining characteristics of cloud computing. Multi-tenant risks include the failure of mechanisms separating the usage of storage, memory, routing and even reputation between different tenants (isolation failure), or the deliberate attempt to subvert those mechanisms (e.g., guest-hopping attacks). At the IaaS level, the consumer may be responsible for security in some multi-tenant situation, such as guest operating system security and firewall configurations.

3.1.4.2 Denial of Service (DoS)

There is debate regarding whether cloud or on-premise infrastructure is more vulnerable to DoS attacks. Some security professionals have argued that the cloud is more vulnerable to DoS attacks because it is shared by many users, which creates potential for more damage per attack. Regardless of which is more vulnerable, both traditional on-premise IT systems and cloud systems can be attacked and therefore must be protected.

3.1.4.3 Decreased Visibility and Control of Physical Infrastructure

The agency must rely on and partner with the CSP to monitor security of the physical infrastructure. This includes all compute, storage and network devices, and also the physical facilities. Agency security personnel and processes must adapt by moving from a direct hands-on role in network security to a management and oversight role of the CSP.

3.1.4.4 Elasticity and On Demand Service Provisioning

Potential changes in system boundaries associated with the elastic expansion of computing and storage capabilities mean there is no longer a pre-defined “perimeter” where applications and data inside are secure. The perimeter is now dynamic, and includes risks from attackers taking advantage of shared memory, processing, or storage. Isolation of virtual machines must include protection from sequential processing risks (i.e., the risk of an attacker gaining information from a previously running application by allocating and reading the same memory locations.)

3.1.4.5 Service Unavailability

This could be caused by a host of factors, from equipment or software failures in the provider's data center, through failures of the communications between the consumer systems and the provider services.[24] The overall cloud design should be inspected to eliminate possible single points of failure. Contingency plans should be developed and tested to address potential service outages.

3.1.5 Other Security Related Considerations[25]

Migrating an agency's systems to a cloud computing environment requires the agency to address security-rooted considerations beyond technical needs. Cloud computing planning activities need to consciously consider these within the new computing paradigm. This section provides an overview of several recurring responsibilities that will also be directly impacted by the security consequences of cloud migration. These include responsibilities for compliance with Privacy, Civil Rights and Civil Liberties (CR/CL), litigation-linked data integrity and availability issues critical to electronic discovery and other forensic issues, and records management including retention requirements and disposition.

3.1.5.1 Electronic Discovery

Electronic Discovery (e-Discovery) refers to legal or government investigations of electronic information, which is also known as Electronically Stored Information (ESI). Relevant data are identified by attorneys and placed on legal hold. Digital forensic procedures extract and analyze the data for evidence. All agencies have experienced requests for information relating to investigations and civil litigation. When documents and other data artifacts are collected in either hard or soft copy, there are specific procedures that must be followed. In executing its cloud strategy, agencies will have to be able to collect, preserve and present ESI in a manner consistent with State and Federal law enforcement. Rules of Evidence, Rules of Procedure, and specific Federal laws govern the storage and presentation of electronic information for law enforcement purposes.

3.1.5.2 Cloud Computing Forensics

Forensic analysis in cloud computing environments presents both opportunities and additional challenges. Some capabilities, such as failover protection, backups, virtual machines, and other safeguards available in most cloud environments can preserve data that might not be recoverable in a traditional environment. For example, an area of concern is the inability to seize physical disks in a cloud environment. However, tools and techniques have been developed that allow forensics to be performed without physical disk seizure. The NIST Cloud Computing Forensic Science Working Group analyzed and categorized numerous possible challenges that fall into technical, legal, or organizational areas, which could impede a digital forensics examiner. They concluded that "more research is required in the cyber domain, especially in cloud computing, to identify and categorize the unique aspects of where and how digital evidence can be found."[26]

[24] Cloud Standards Customer Council, *Security for Cloud Computing: 10 Steps to Ensure Success*, Aug 2012

[25] Eiben, K. VA Cloud Computing Security Analysis, January 12, 2015

[26] Draft NISTIR 8006, NIST Cloud Computing Forensic Science Challenges, NIST Cloud Computing Forensic Science Working Group, Information Technology Laboratory, June 2014, http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

3.1.5.3 Geographic Considerations

Federal cloud environments cannot store data outside of the geographic boundaries of the United States, or specifically designated overseas locations, such as military bases.

3.1.5.4 Privacy and Civil Rights/Civil Liberties (CR/CL)

Properly addressing the Privacy and CR/CL issue in the era of cloud services adds a layer of inquiry to the examination of agency data system management. The practices of the CSP must be included when assessing the agency's Privacy and CR/CL practices. As necessary, specific contract language should be included to clarify the agency's retention of statutory responsibility for privacy compliance and the CSP's operating obligations over data, including special considerations applicable to stewardship of Personally Identifiable Information (PII) and Protected Health Information (PHI).

3.1.5.5 Meeting Office of the Inspector General (OIG) Cloud Computing Requirements

As the agency moves into a cloud computing environment, OIG must retain the ability to appropriately access the information required to perform their investigative responsibilities. In a cloud computing environment, however, where allocation of the responsibility and mechanism for providing access to any information can become a challenge, assuring any particular organization access requires specific contract language to support that access. Depending on the cloud service, the agency resources may not have operational responsibility for managing the environment of the files captured, stored, or processed within them. That delegation does not, however, eliminate the need for the agency OIG to have appropriate access to the information. Nor does it necessarily mean the same techniques must be supported to providing access to information required to perform oversight (e.g., physically accessing computing resources such as hard disk drives).

3.1.5.6 Acquisition Documents

Appropriate acquisition documentation (e.g., contracts, statements of work) must include security requirements and the extent to which the agency's CSPs must be held accountable for data custody. SLAs should be documented between the agency consumer and the CSP to ensure clear understanding of the security measures, expected performance or outcomes, and consequences for failing to meet them. SLAs also provide the opportunity to encourage desired behaviors by establishing rewards for exceptional performance. Security requirements and SLAs must align to Federal law, agency policy, and practical standards, including security related concerns such as OIG access, audits, reporting, and exit parameters in the event the relationship with the CSP is terminated.

4 Cloud Security Guidance[27]

As agencies transition their applications and data to cloud computing solutions, it is critically important that the level of security provided in the cloud environment be equal to or better than the security provided by their traditional IT environment. This section discusses some overall security steps that can be taken to plan for and manage security while adopting cloud computing.

4.1 Security Strategy

A comprehensive and clear cloud security strategy will provide a needed foundation for securing the agency's cloud adoption. The security strategy should align with the cloud adoption strategy, the overall IT strategy, and the overall IT security strategy.

The cloud security strategy should address both technical and non-technical aspects of security, and provide an overall framework for securing the entire cloud ecosystem. It must also ensure security across the responsibility boundaries of the multiple agency organizations, and multiple CSPs. Often, agency systems also interface or integrate with other Federal, State, Local or Tribal government entities, as well as the American public. The cloud security strategy must account for security of cloud within all scenarios, and across them. Some topics for a cloud security strategy include (but are not limited to):

- Mission goals and objectives for cloud security
- Evaluating cloud security readiness, including comprehensive security policy review
- How FedRAMP fits into the agency's approach
- Approach for integrating security across the cloud ecosystem
- Approach for integrating traditional security and cloud security
- Approach for continued security of legacy systems moved to cloud
- Identifying resources impacted by cloud deployments and engaging them in security
- Cloud acquisition considerations and approach for security

4.2 Systems Categorization

In accordance with the NIST Risk Management Framework, agency system owners are required to categorize their information systems as Low, Moderate, or High. The system categorization is derived from the three security objectives of confidentiality, integrity, and availability. NIST provides guidance for categorizing the information system based on the data and capabilities provided by the system.[28] System categorization has to be based on the standards defined in Federal Information Processing Standards Publication 199[29] (FIPS PUB 199).

Table 4-1 shows the approximate number of security controls that are allocated to each categorization baseline and the total number of controls available in the NIST catalog. The system categorization drives the baseline of security controls that apply to a system, thus as the system categorization increases, so does the number of security controls that must be applied to the system. Similarly, there is a direct relationship between the number of controls and the effort

[27] Cloud Standards Customer Council, *Security for Cloud Computing: 10 Steps to Ensure Success*, Aug 2012

[28] FIPS 199 and guidance based on it provide extensive discussion of the methodology and rationale for categorization process.

[29] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

that must be applied to implementing them. Therefore, the greater the number of controls, the greater the cost of securing the system at that level.

Table 4-1 Total Security Controls by Baseline

Security Control Baseline	Control Count
Low	523
Moderate	721
High	832
Total Available	1,492

Over-categorizing an information system can lead to increased cost due to added security controls and increased scrutiny from oversight organizations. Over categorization can also negatively impact processes if the higher level baselines are fully implemented. The effect of over categorization could lead to the acquisition of private clouds that may not fully utilize all of the benefits associated with a cloud solution. Agencies can establish a clearly-defined system categorization and validation program, which should include a re-validation schedule at least annually, in which applications and systems are re-evaluated for their sensitivity and criticality. This would avoid unnecessary restrictions on cloud adoption, and provide cost savings, while continuing to maintain adequate security for all systems.

4.3 Review Security Policy

Many agencies' policies are designed for traditional IT enterprises, and may not adequately support cloud adoption. Specifically, some agencies must align with FedRAMP and Trusted Internet Connections[30] (TIC) 2.0[31] (or upcoming 3.0) requirements and controls.

For example, the TIC 2.0 guidelines expressly permit departments and agencies to extend their internal computing capabilities to a FedRAMP CSP without requiring either a dedicated circuit, or the implementation of a physical "air-gap." The TIC 2.0 guidelines also do not require that intra-agency connections traverse a TIC gateway, when the FedRAMP cloud instance is not publicly accessible and does not host non-federal tenants. These latter conditions would be satisfied by a CSP who offers a FedRAMP-certified federal community cloud.

The agency needs to formulate a cloud security strategy that satisfies both the security goals of TIC 2.0 and FedRAMP.

4.4 Security Requirements of the Exit Process

The exit process or termination of the use of a cloud service by a consumer requires careful consideration from a security perspective.

During the exit process, the agency consumer should receive a smooth transition, regaining all data and applications (as appropriate) without loss or security breach. Thus the exit process must allow the consumer to retrieve their data in a suitably secure form, backups must be retained for

[30] http://www.dhs.gov/trusted-internet-connections
[31] https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf

agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.[32]

Within the boundaries of legal requirements for data retention, it is important that once the consumer has completed the termination, "reversibility" or "the right to be forgotten" is achieved (i.e. all data should be returned to the agency, and none should remain with the CSP).[33] Note that if legal requirements impose data retention on the CSP, the agency's data should be completely removed to off-line storage devices away from the active physical infrastructure. For all practical purposes, the data should be completely inaccessible to any cloud users, and minimally accessible by CSP personnel.

[32] Cloud Standards Customer Council, *Security for Cloud Computing: 10 Steps to Ensure Success*, Aug 2012
[33] Cloud Standards Customer Council, *Security for Cloud Computing: 10 Steps to Ensure Success*, Aug 2012

Appendix A Federal Risk and Authorization Management Program (FedRAMP)[34]

The General Services Administration, as the Federal government's generic authority for management of information technology policy and practices across civilian agencies, is responsible for implementation of FedRAMP. FedRAMP is a government-wide program that provides a standardized approach to the security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP utilizes a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant agency security assessments.[35] Where the agency requirements and mission needs support the use of specific cloud services (IaaS, PaaS, or SaaS), services with a current FedRAMP PATO should be included in the total set of products and services evaluated. The potential for cost reduction, which includes meeting baseline security requirements, should be addressed in the agency IT procurement guidance.

GAO has described the purposes of FedRAMP to be:

- Ensure that cloud based services have adequate information security;
- Ensure FedRAMP supports all needed security control baselines; currently it supports Low and Moderate baselines;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies.

Additionally, continuous monitoring provides risk visibility into and across FedRAMP approved services while assisting CSPs to maintain secure baselines over time. This also provides a risk framework that could identify and report security breaches (if/when they occur) to the United Stated Computer Emergency Readiness Team (US CERT) in a timely manner.

[34] Credit to Eiben, K. VA Cloud Computing Security Analysis, January 12, 2015

[35] http://cloud.cio.gov/faq/what-fedramp

Appendix B Risk Management Framework[36]

A risk-based approach to security control selection and specification needs to consider effectiveness, efficiency, and the constraints imposed by laws, directives, guidelines, and policies. While the original NIST RMF provides a flexible approach, it is aimed at addressing issues associated with a traditional IT environment. More recently, the NIST Cloud Computing Security Working Group has customized the traditional RMF in order to better address the challenges posed by cloud-based services.[37] The Cloud-adapted RMF (CRMF) closely parallels the original RMF, and consists of the following six steps:

Step 1: **Categorize** the information system or service migrated to the cloud, and the information processed, stored, and transmitted by that system based on an analysis of the impact produced by a compromise. This step is very similar to the first step of the original RMF. The importance of this step cannot be overstated, because categorization provides the basis for actions that are taken in subsequent steps of the framework. NIST has defined impact levels for the compromise of information confidentiality, integrity, and availability in FIPS PUB 199, and these are presented in Table B-1.

Table B-1. Impact Levels for Confidentiality and Integrity

Security Objective	Potential Impact		
	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

[36] Credit to Eiben, K. VA Cloud Computing Security Analysis, January 12, 2015
[37] NIST SP 500-299 (draft), op cit.

While FIPS PUB 199 has been a mandatory federal standard for many years, it is rarely used effectively to manage the risk associated with federal information assets. All too often, federal agencies adopt informal policies that result in defining whole classes of mission-related systems as being in the high category. This approach is not consistent with FIPS PUB 199.

Step 2: **Identify** security requirements for the information system or service being migrated to the cloud. This involves using the outcome of Step 1 and combining it with estimates of other risk factors that are applicable (e.g., threat-level analysis) to identify the security components that are most appropriate for the system in question. Select the baseline security controls.

Step 3: **Select** the cloud ecosystem architecture that best fits the analysis performed in Step 2 for the information system or service that will be migrated to the cloud.

Step 4: **Assess** cloud service provider(s) based on their Authorization-To-Operate (ATO). Compare the security controls needed for the cloud-based system against those controls that have already been implemented by the cloud provider. Negotiate the implementation of any additional security controls that are deemed to be necessary for the system/service. In addition, identify the security controls that are the agency's responsibility, and implement them.

Step 5: **Authorize** the use of the selected cloud provider (and cloud broker, when applicable) for hosting the cloud-based information system or service. Negotiate a Service Agreement (SA) and SLA that incorporates the results of the negotiation performed in Step 4.

Step 6: **Monitor** the cloud provider (and the cloud broker when applicable) to ensure that all SA and SLA terms are met and that the cloud-based information system maintains the necessary security posture. Directly monitor the security controls that the agency has implemented.

The cloud risk management framework provides a set of fundamental steps that the agency system owners should use to plan, acquire, and operate secure cloud-based computing environments.

Appendix C Cloud Authorization to Operate[38]

The NIST RMF provides guidance for accreditation of all IT systems. FedRAMP applies the same framework for assessment and authorization with controls that are specific to cloud. Figure 4-1 shows the security control selection process.

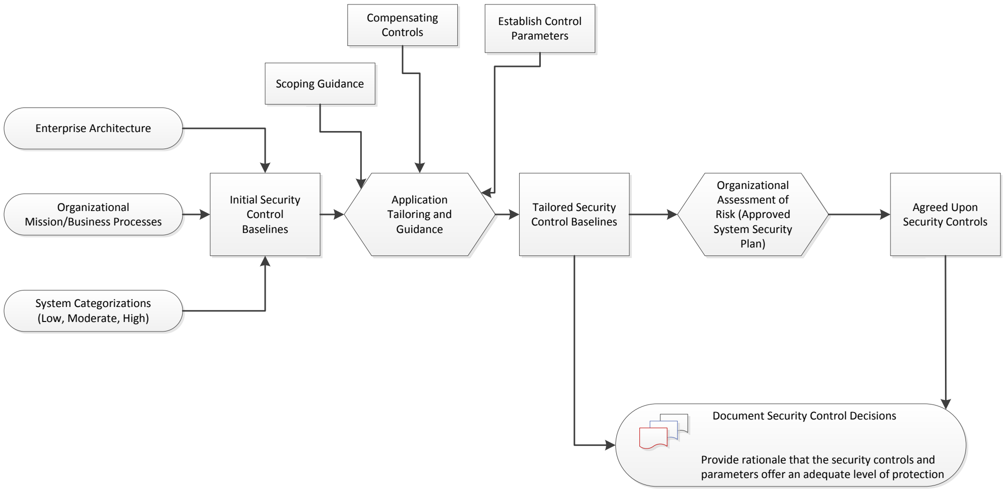

Compensating Controls
Establish Control Parameters
Scoping Guidance
Enterprise Architecture
Organizational Mission/Business Processes
System Categorizations (Low, Moderate, High)
Initial Security Control Baselines
Application Tailoring and Guidance
Tailored Security Control Baselines
Organizational Assessment of Risk (Approved System Security Plan)
Agreed Upon Security Controls
Document Security Control Decisions
Provide rationale that the security controls and parameters offer an adequate level of protection

Figure C-1. Security Control Selection Process

Although FedRAMP has a defined set of paths for cloud authorization, agencies are encouraged to define mission specific controls that will augment the FedRAMP security control baselines.

There are three authorization paths defined by the FedRAMP Program Management Office:

- Provisional ATO;
- Federal Agency ATO; and
- CSP-Supplied security package.

Figure C-2 shows the three FedRAMP authorization paths.

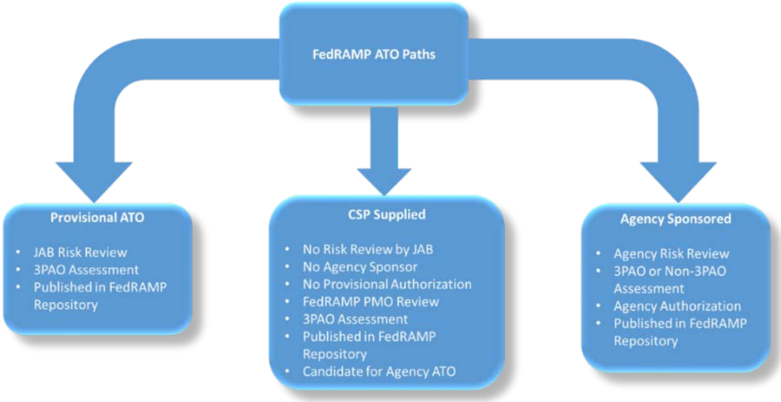


Figure C-2. FedRAMP Authorization Paths

[38] Credit to Eiben, K. VA Cloud Computing Security Analysis, January 12, 2015

Provisional Authorization to Operate (PATO): A CSP submits a documentation package to the FedRAMP Program Management Office (PMO) for review. The Joint Authorization Board (JAB) grants a provisional authorization, and the cloud offering documentation package is uploaded to the FedRAMP repository so that it can be leveraged by government agencies.

Agency Sponsored Authorization to Operate (ATO): A CSP submits an authorization package to a specific agency. The agency leverages the documentation for issuing their own agency ATO. Other agencies can leverage this ATO once it is published in the FedRAMP repository.

CSP Supplied: A CSP can submit a package for FedRAMP PMO review without having agency sponsorship. The CSP will have to have an independent assessment performed by an approved 3PAO, but the CSP does not receive a P-ATO. The end result is a package that is submitted into the FedRAMP repository with assessment activity performed. The CSP then becomes a candidate for sponsorship.

Leveraging the FedRAMP ATO paths, to align the controls of existing and candidate CSPs with those from agency security policies, the agency will have to review the CSP's security controls. There are two FedRAMP documents that the CSP should have as part of their authorization package.

- **Cloud Tailoring Workbook (CTW)**: Defines the security control configuration parameters the CSP has implemented. Provides a rationale for controls that are either met, not met, or mitigated with a compensating control.
- **Control Implementation Summary (CIS)**: Assigns responsibility for implementing each security control. The CIS control assignment can fall into one of the categories shown in **Table 4-2. Security Control Assignment Categories**[39]:

Table 5-1. Security Control Assignment Categories

Assignment Category	Description
Service Provider Corporate	A common control provided by the CSP.
Service Provider System Specific	A unique control specific to the cloud offering.
Service Provider Hybrid	A combination of Service Provider Corporate and Service Provider System Specific. The CSP is still solely responsible for implementing this type of control.
Configured by Customer	A customer-provided parameter value or activity (profiles, configurations, and numeric values or ranges).
Provided by the Customer	Additional software or hardware is required from the Customer in order to meet the control (e.g., two-factor authentication requirements).
Shared	A control that is implemented by both the CSP and the Customer.
Inherited	A control that is inherited from an existing provisional authorization.

[39] FedRAMP Control Implementation Summary Template. http://cloud.cio.gov/document/control-implementation-summary

If the agency has an existing relationship with a CSP, it can request a review of the CSP's documentation, provided the CSP has FedRAMP-formatted artifacts. FedRAMP recommends that agencies review existing contracts for FedRAMP provisions, determine from each CSP their intent to obtain FedRAMP provisional authorization, and to have CSPs migrate their current security documents over to FedRAMP-supplied templates.[40]

Through a review of the CTW and CIS documents, the agency will understand the alignment of security control assignments. Further allocation assignment will be necessary for agency-specific controls. The agency must also review the residual risks identified in the CSP authorization package to determine whether these risks are acceptable enough for the application that will be hosted in the cloud.

Ultimately the agency is responsible for the authorization of the application hosted in the cloud, which includes accepting any residual risk that is not mitigated with the CSP.

[40] Guide to Understanding FedRAMP Version 2.0; June 6, 2014.

Appendix D NIST Guidance and Policy Publications[41]

Publication Number	Title	Description/Purpose
NIST Special Publication 800-144.	Guidelines on Security and Privacy in Public Cloud Computing, December 2011	An overview of the privacy and security risks observed in public clouds.
NIST Special Publication 800-145	NIST Definition of Cloud Computing, September 2011	This publication provides the definitive terms for the Service Models and Deployment Models. By declaring standard terminology for cloud computing, agencies now have the ability to formulate a strategy using common terms.
NIST 800-146	Cloud Computing Synopsis and Recommendations, May 12, 2011	This document covers the risks and benefits of using the cloud. It provides recommendations on how to encounter inherent risks to cloud computing.
NIST 500-291	NIST Cloud Computing Standards Roadmap, August 10, 2011	The Roadmap gives agencies the tools they need to adopt could computing. It imports the best practices from industry, academia, and oversight agencies to ensure that those agencies who are looking to deploy a cloud are making well informed decisions on risks and benefits.
NIST 500-292	NIST Cloud Computing Reference Architecture, September 2011	The reference architecture, as defined below, describes the cloud ecosystem and serves as a model upon which other agencies can build their cloud program.
NIST 500-293	US Government Cloud Computing Technology Roadmap, Release 2.0, July 2013	The Roadmap is a three-volume set that serves to provide the material needed for agencies who are trying to incorporate cloud computing into their environment but lack the knowledge needed for migration. It is intended to provide the material needed to make sound decisions for migrating to the cloud.
NIST Special Publication 500-293, Volume I and Volume II	US Government Cloud Computing Technology Roadmap	Volume I covers the ten requirements necessary for an agency to adopt a cloud. These requirements cover security, interoperability, portability, performance and accessibility. The Cloud Computing Reference Architecture is depicted Volume II along with a taxonomy and use cases. The use cases are both technical and business in nature. The intention of this volume is to provide background material for agencies to use when they are considering cloud adoption

[41] Credit to Eiben, K. VA Cloud Computing Security Analysis, January 12, 2015

Publication Number	Title	Description/Purpose
NIST Interagency Report 7956	Cryptographic Key Management Issues & Challenges in Cloud Services, September 2013	This report discusses the challenges involved in deploying cryptographic key management functions that meet the security requirements of the cloud customer.
NIST Interagency Report 7904	DRAFT Trusted Geolocation in the Cloud: Proof of Concept Implementation; December 21, 2012	There is concern over the location of cloud resources in foreign countries. This publication covers the concerns with an IaaS implementation that was proposed to address some of the concerns and operational challenges with co-location.
NIST Interagency Report 8006	DRAFT NIST Cloud Computing Forensic Science Challenges; June 23, 2014	This is a draft publication on the challenges encountered while investigating incidents that occurred in a cloud. It provides insight into the forensic science concerns as identified by the NIST Cloud Computing Forensic Science Working Group.
ITL March 2012 ITL June 2012	Information Technology Bulletins from March and June 2012	These bulletins announced the cloud computing publications for the year and provided links to the FedRAMP site.

Appendix E Acronyms

Term	Definition
3PAO	Third Party Assessment Organization
A&A	Assessment and Authorization
ATO	Authorization to Operate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIS	Control Implementation Summary
COTS	Commercial Off the Shelf
CR/CL	Civil Rights/Civil Liberties
CRMF	Cloud-adapted Risk Management Framework
CSC	Cloud Service Consumer
CSP	Cloud Service Provider
DHS	Department of Homeland Security
e-Discovery	Electronic Discovery
EDRM	Electronic Discovery Reference Model
EO	Enterprise Operations
E-Records	Electronic Records
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
GAO	Government Accountability Office
HIPAA	Health Information Portability and Accountability Act
IA	Information Assurance

Term	Definition
IaaS	Infrastructure as a Service
IG	Inspector General
IT	Information Technology
JAB	Joint Authorization Board
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
PaaS	Platform as a Service
PATO	Provisional Authorization to Operate
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RMF	Risk Management Framework
SaaS	Software as a Service
SLA	Service Level Agreement
SP	Special Publication
TAC	Technology Acquisition Center
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Provider
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network